Algèbre M1 Cours 8

Théorie de Galois

9 Novembre 2010

Problématique

Soit K une extension de k. On cherche à comprendre la structure d'extension de K et pour cela à déterminer toutes les sous-k-extensions de K. Même si $[K : k] < +\infty$, K peut avoir une infinité de sous-extension : en effet, on a vu que pour une extension finie, le nombre de sous-extension est finie si et seulement l'extension est monogène ; de plus on a vu qu'une extension séparable est toujours toujours monogène. Ainsi, il est raisonnable de ne considérer que les extensions séparables.

Par ailleurs, une façon de produire des sous-extensions de K est de considérer les sous-extensions de la forme

$$K^H = \{x \in K, \qquad \forall \sigma \in H, \quad \sigma(x) = x\}$$

où H est une sous-groupe de $G = \mathrm{Gal}(K/k) = \mathrm{Aut}_k(K)$.

Pour avoir une chance de décrire toutes les sous-extensions de K par cette méthode, il faut que G soit aussi gros que possible c'est-à-dire que $|G| = [K : k]_{\mathrm{s}}$ et on a vu que cette condition signifiait que K était une extension normale de k (au moins si $[K : k]_{\mathrm{s}}$ était finie).

Problématique (suite)

En effet, pour $j : K \to \Omega$, l'application

$$\begin{cases} G \longrightarrow \mathrm{Hom}_{k-\mathrm{ext.}}(K, \Omega) \\ \sigma \longmapsto j \circ \sigma \end{cases}$$

est injective.
Finalement, les extensions qui vont nous intéresser sont les extensions à la fois normale et séparable.

Définition – Extension galoisienne. Soit $(K : k)$ une extension. On dit que K est une *extension galoisienne* de k si K est une extension normale et séparable de k.

Extension galoisienne

Proposition – Caractérisation des extensions galoisiennes.
Soit K une extension algébrique de k. On note $G = \mathrm{Gal}(K/k)$. Les propositions suivantes sont équivalentes

(i) K est une extension galoisienne de k

(ii) $K^G = k$

(iii) Tout polynôme irréductible sur k ayant une racine dans K est scindé à racine simple dans K

(iv) Pour tout $x \in K$, le polynôme minimal de x sur k se factorise dans $K[X]$ en produit de polynômes distincts de degré 1

(v) K est le corps de décomposition d'une famille $\mathscr{F}$ de $k[X]$ formées d'éléments P vérifiant $\mathrm{pgcd}\,(P, P') = 1$.

De plus si $[K : k] < +\infty$, les conditions précédentes sont équivalentes à

(vi) $|G| = [K : k]$.

Preuve

$(iii) \Leftrightarrow (iv)$. Un polynôme irréductible sur k ayant une racine dans K est proportionnel au polynôme minimal de cette racine. Inversement, le polynôme minimal de $x \in K$ est irréductible sur K et admet une racine dans K.

$(i) \Rightarrow (v)$. K est normal sur k donc K est le corps de décomposition de la famille des polynômes irréductibles sur k ayant une racine dans K ou ce qui revient au même de la familles des polynômes minimaux sur k des éléments de K. Comme K est séparable sur k ces polynômes sont séparables et donc $\mathrm{pgcd}\,(P, P') = 1$.

$(v) \Rightarrow (i)$. K est normale puisque c'est un corps de décomposition. De plus, K est engendrée sur k par les racines des éléments de $\mathscr{F}$. Or le polynôme minimal d'une racine d'un élément de $\mathscr{F}$ est séparable car il divise un élément de $\mathscr{F}$ et que les éléments de $\mathscr{F}$ sont à racines simples dans une extension suffisamment grande. Ainsi K est engendrée sur k par des éléments séparables et donc K est séparable sur k.

Preuve (suite)

$(i) \Rightarrow (iii)$. Tout polynôme irréductible P sur k ayant une racine dans K est scindé puisque K est normale. Comme P est le polynôme minimal d'une de ces racines dans K et que K est séparable sur k alors P est séparable et donc à racines simples dans K.

$(iii) \Rightarrow (i)$. Tout polynôme irréductible sur k ayant une racine dans K étant scindé dans K, l'extension $(K : k)$ est normale. De plus le polynôme minimal d'un élément $x \in K$ est irréductible sur k et a une racine dans K donc est à racines simples dans K et il est donc séparable. Ainsi $(K : k)$ est séparable.

Preuve : le cas (ii)

$(i) \Rightarrow (ii)$. On a bien sûr $k \subset K^G$ puisque tous les éléments de G sont k-linéaires. On fixe à présent une extension algébriquement close Ω de K contenant K. Si $x \in K \smallsetminus k$ le polynôme minimal de x sur K est de degré supérieur ou égal à 2 et admet donc une racine y distincte de x puisque x est séparable sur k. Il existe alors un (unique) k-morphisme $\tau : k(x) \to \Omega$ tel que $\tau(x) = y$. Ce morphisme se prolonge en un morphisme $\sigma : K \to \Omega$. De plus, comme K est normale sur k, on a $\sigma(K) = K$ et $\sigma \in \mathrm{Gal}(K/k)$. Ainsi, si $x \notin k$ alors il existe $\sigma \in \mathrm{Gal}(K/k)$ tel que $\sigma(x) = y \neq x$.
$(ii) \Rightarrow (iv)$. Soit $x \in K$ et P le polynôme minimal de x sur k. On note $x = y_1, \ldots, y_\ell$ les racines distincts de P dans K et $Q = (X - y_1) \cdots (X - y_\ell)$. Pour tout $g \in G$, il existe j tel que $gy_i = y_j$ (g envoie les racines de P sur les racines de P). On en déduit que $Q \in K^G[X]$ et donc $Q \in k[X]$. Comme $Q \mid P$ et $P \in k[X]$ est irréductible , on en déduit que $P = Q$ est scindé à racines simples dans K.

Preuve : extension finie

Pour une extension finie, on a $|G| \leqslant [K : k]_{\mathrm{s}} \leqslant [K : k]$. De plus, on a $|G| = [K : k]_{\mathrm{s}}$ si et seulement si K est normale (puisque $[K : k]_{\mathrm{s}}$ est fini) et $[K : k]_{\mathrm{s}} = [K : k]$ si et seulement si l'extension $(K : k)$ est séparable.

Remarque – Extension finie galoisienne. Soit $(K : k)$ une extension finie. On a déjà vu que L'extension $(K : k)$ est galoisienne si et seulement si K est le corps de décomposition d'un polynôme irréductible séparable.

Correspondance

Soit K une extension algébrique de k. On note $\mathscr{E}$ l'ensemble des sous-k-extensions de K et $\mathscr{G}$ l'ensemble des sous-groupes de $G = \mathrm{Gal}(K/k)$.

Si $H \in \mathscr{G}$, on a vu que $K^H := \{x \in K, \quad \forall \sigma \in H, \quad \sigma(x) = x\}$ est une sous-extension de K. On définit ainsi une application $\Phi : H \in \mathscr{G} \mapsto K^H \in \mathscr{E}$.

Inversement, si $E \in \mathscr{E}$ l'ensemble des $\sigma \in G$ tel que $\sigma(x) = x$ pour tout $x \in E$ est un sous-groupe de G qui n'est autre que $\mathrm{Gal}(K/E)$. On définit ainsi une application $\Gamma : E \in \mathscr{E} \mapsto \mathrm{Gal}(K/E) \in \mathscr{G}$.

Dans la suite, on va étudier ces applications. Par exemple, on a déjà vu que $\Phi(G) = k$ si et seulement si K est galoisienne.

ATTENTION!!! Si $k \subset E \subset K$ est une suite d'extension, on a $\mathrm{Gal}(K/E) \leqslant \mathrm{Gal}(K/k)$ mais on n'a pas $\mathrm{Gal}(E/k) \subset \mathrm{Gal}(K/k)$. On verra que dans certains cas, $\mathrm{Gal}(E/k)$ est un quotient de $\mathrm{Gal}(K/k)$.

Premières propriétés

Proposition Soient $E, E_1, E_2 \in \mathscr{E}$ et $H, H_1, H_2 \in \mathscr{G}$, on a alors les propriétés suivantes

(i) si $E_1 \subset E_2$ alors $\Gamma(E_2) \subset \Gamma(E_1)$

(ii) si $H_1 \subset H_2$ alors $\Phi(H_2) \subset \Phi(H_1)$

(iii) $E \subset \Phi(\Gamma(E))$

(iv) $H \subset \Gamma(\Phi(H))$

(v) $\Phi \circ \Gamma \circ \Phi = \Phi$ et $\Gamma \circ \Phi \circ \Gamma = \Gamma$

(vi) Pour $\sigma \in G$, on a

$$\Gamma(\sigma(E)) = \sigma\Gamma(E)\sigma^{-1} \qquad \text{et} \qquad \Phi(\sigma H \sigma^{-1}) = \sigma(\Phi(H)).$$

Preuve. (i) Un élément qui vaut l'identité sur E_2 vaut l'identité sur E_1.

(ii) Un élément qui est fixe par tous les éléments de H_2 est fixe par tous les éléments de H_1.

Preuve

(iii) Un élément de E est fixe par tous les éléments du groupe de Galois de K sur E.

(iv) Un élément de H laisse fixe tous les éléments de K^H et donc est dans le groupe de Galois de K sur K^H.

(v) On a $\Phi(H) \subset \Phi \circ \Gamma(\Phi(H))$ d'après (iii). De plus, on a $H \subset \Gamma(\Phi(H))$ d'après (iv) et donc $\Phi(\Gamma(\Phi(H)) \subset \Phi(H)$ d'après (ii).
On a $\Gamma(E) \subset \Gamma \circ \Phi(\Gamma(E))$ d'après (iv). De plus, on a $E \subset \Phi(\Gamma(E))$ d'après (iii) et donc $\Gamma(\Phi(\Gamma(E)) \subset \Gamma(E)$ d'après (i).

(vi) $g \in \Gamma(\sigma(E))$ si et seulement si $g\sigma(x) = \sigma(x)$ pour tout $x \in E$ si et seulement si $\sigma^{-1}g\sigma(x) = x$ pour tout $x \in E$ si et seulement si $\sigma^{-1}g\sigma \in \Gamma(E)$.
$x \in \Phi(\sigma H \sigma^{-1})$ si et seulement si $\sigma h \sigma^{-1}(x) = x$ pour tout $h \in H$ si et seulement si $h\sigma^{-1}(x) = \sigma^{-1}(x)$ pour tout $h \in H$ si et seulement si $\sigma^{-1}(x) \in K^H$.

Caractérisation de l'image

Proposition Soit $E \in \mathscr{E}$. On a équivalence entre

(i) E est dans l'image de Φ
(ii) $\Phi(\Gamma(E)) = E$
(iii) K est une extension galoisienne de E

Proposition Soit $H \in \mathscr{G}$. On a équivalence entre

(i) H est dans l'image de Γ
(ii) $\Gamma(\Phi(H)) = H$

Corollaire – Bijection. Γ et Φ induisent par restriction des bijections inverses l'une de l'autre entre l'image l'image de Φ et l'image de Γ.

Preuve

Preuve. Si $\Phi(\Gamma(E)) = E$ alors E est dans l'image de Φ. Si $E = \Phi(H)$, on a bien $E = \Phi(H) = \Phi\Gamma(\Phi(H)) = \Phi(\Gamma(E))$. On a $\Phi(\Gamma(E)) = K^{\mathrm{Gal}(K/E)}$. Ainsi $E = \Phi(\Gamma(E))$ si et seulement si $K^{\mathrm{Gal}(K/E)} = E$ si et seulement si K est une extension galoisienne de E (car K est une extension algébrique de E).

Si $H = \Gamma(\Phi(H))$ alors H est dans l'image de Γ. Si $H = \Gamma(E)$ alors $H = \Gamma(E) = \Gamma\Phi\Gamma(E) = \Gamma\Phi(H)$.

Remarque – Le cas d'une extension galoisienne. On suppose que $(K : k)$ est galoisienne. Alors toute extension E est dans l'image de Φ. En effet, $(K : E)$ est galoisienne par transitivité de la séparabilité et « ce qu'il reste de la transitivité pour les extensions normales ».

Problème : trouver une caractérisation de l'image de Γ

$\longrightarrow$ topologie de Krull

Le lemme d'Artin

Proposition – Lemme d'Artin. Soit L un corps et H un sous-groupe fini du groupe des automorphismes de L. Alors L est une extension galoisienne de L^H de degré $|H|$ et de groupe de galois H.

Corollaire Tout sous-groupe fini H de $\mathrm{Gal}(K/k)$ est dans l'image de Γ : en effet, d'après le lemme d'Artin, $H = \mathrm{Gal}(K/K^H)$.

Preuve du lemme d'Artin

Soit $x \in L$. On note $\{x_1 = x, x_2, \ldots, x_\ell\} = \{hx,\ h \in G\}$ l'orbite de x sous l'action du groupe H avec $x_i \neq x_j$ si $i \neq j$. Le polynôme $Q(X) = (X - x_1) \cdots (X - x_\ell) \in L^H[X]$ est à racine simple et annule x. Ainsi x est algébrique et même séparable sur L^H et $(L : L^H)$ est séparable.

Par ailleurs, si P est le polynôme minimal de x sur L^H et $h \in H$. On a $P(hx) = h(P(x)) = 0$. Ainsi les x_i sont aussi racines de P et donc $Q \mid P$. Comme P est irréductible, on a $Q = P$. Le polynôme minimal de x est donc scindé dans L et $(L : L^H)$ est une extension normale.

L'extension $(L : L^H)$ est bien galoisienne.

Montrons à présent que $[L : L^H] \leqslant |H|$. On a vu que c'est le cas pour toute sous-L^H-extension monogène de L : $[L^H(x) : L] \leqslant |H|$ pour tout $x \in L$. Si $[L : L^H] < +\infty$ alors $[L : L^H] < |H|$ car L est monogène car séparable et finie sur L^H. Si $[L : L^H] = +\infty$, il existe $|H| + 1$ éléments algébriquement L^H-indépendants dans L. L'extension engendrée par ces éléments est alors finie (puisque algébrique et de type fini) et séparable sur L^H donc monogène. Ainsi son degré sur L^H est majoré par $|H|$ ce qui est absurde.

On a alors $[L : L^H] \leqslant |H| \leqslant \mathrm{Gal}(L/L^H) \leqslant [L : L^H]$. La deuxième inégalité résulte du fait que $H \subset \mathrm{Gal}(L/L^H)$, la troisième inégalité du fait que $[L : L^H]$ est fini. On en déduit alors que $H = \mathrm{Gal}(L/L^H)$ et $|H| = [L : L^H]$.

Le théorème de correspondance de Galois

Théorème Soit $(K : k)$ une extension galoisienne **finie**. Les applications Φ et Γ définissent des bijections réciproques l'une de l'autres entre l'ensemble $\mathscr{E}$ des sous-k-extensions de K et l'ensemble $\mathscr{G}$ des sous-groupes de $G = \mathrm{Gal}(K/k)$.

Dans cette bijection le degré sur k et l'indice se correspondent : si $E = K^H$ ou $H = \mathrm{Gal}(K/E)$, on a $|H| = [K : K^H]$ et $|G| = [K : K^G] = [K : k]$. Ainsi par multiplicativité, on a $(G : H) = [K^H : k]$.

Preuve. On a vu que tout sous-extension E de K est telle que $(K : E)$ est galoisienne et est donc dans l'image de Φ. De plus, comme G est fini, tout sous-groupe de G est dans l'image de Γ. Enfin Φ et Γ sont des bijections réciproques l'une de l'autre entre l'image de Γ et l'image de Φ.

Correspondance (suite)

Proposition – Complément à la correspondance. Soit $(K : k)$ une extension galoisienne **finie** de groupe G. On considère H un sous-groupe de G et E une sous-k-extension de K qui se correspondent dans la bijection précédente c'est-à-dire $H = \mathrm{Gal}(K/E)$ et $E = K^H$.
On a les équivalences

(i) H est distingué dans G
(ii) $(E : k)$ est normale
(iii) $(E : k)$ est galoisienne
(iv) $\sigma(E) = E$ pour tout $\sigma \in G$

Dans ce cas, le groupe de Galois $\mathrm{Gal}(E/k)$ s'identifie par l'application restriction à G/H.

Preuve du complément

$(ii) \Leftrightarrow (iii)$. Comme $(E : k)$ est séparable (puisque $(K : k)$ l'est), $(E : k)$ est normale si et seulement si $(E : k)$ galoisienne.

$(i) \Leftrightarrow (iv)$. Comme Φ et Γ sont des bijections inverses l'une de l'autre « compatible avec l'action de G », on a $\sigma(E) = E$ pour tout $\sigma \in G$ si et seulement si
$H = \Phi(E) = \Phi(\sigma(E)) = \sigma\Phi(E)\sigma^{-1} = \sigma H \sigma^{-1}$ pour tout $\sigma \in G$.

$(iii) \Rightarrow (i)$. Si $(E : k)$ galoisienne alors on peut définir le morphisme de groupe

$$r : \begin{cases} \mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(E/k) \\ \qquad \sigma \qquad \longmapsto \sigma_{|E} \end{cases}$$

En effet, $\sigma(E) = E$ car $(E : k)$ est normale. Le noyau de r est $H = \mathrm{Gal}(K/E)$ qui est donc distingué dans G.

Fin de la preuve

$(iv) \Rightarrow (iii)$. Par hypothèse le morphisme r est bien définie et de noyau H. On en déduit que G/H s'identifie à un sous-groupe de $\mathrm{Gal}(E/k)$. Ainsi $|G/H| = [E : k] \leqslant |\mathrm{Gal}(E/k)|$. Comme $|\mathrm{Gal}(E/k)| \leqslant [E : k]$, on en déduit que $|\mathrm{Gal}(E/k)| = [E : k]$ et E est galoisienne.

Lorsque les propriétés sont vérifiées, on obtient par cardinalité que r est surjective et ainsi r définit par passage au quotient un isomorphisme entre G/H et $\mathrm{Gal}(E/k)$.

Exercice – Surjectivité de r. À l'aide du lemme du prolongement de la normalité de E, donner une autre démonstration de la surjectivité de r.

Groupe de Galois et permutation

Soit $P \in k[X]$ un polynôme dont tous les facteurs irréductibles sont séparables. Le corps de décomposition de P sur k noté $D_k(P)$ est alors une extension galoisienne de k et on note $\mathrm{Gal}_k(P) := \mathrm{Gal}(D_k(P)/k)$ le groupe de Galois de P.

Soient $\mathrm{Rac}(P) = \{x_1, \ldots, x_n\}$ l'ensemble des racines de P. Pour $\sigma \in \mathrm{Gal}_k(P)$ et x_i une racine de P, on a $P(\sigma(x_i)) = \sigma(P(x_i)) = 0$. On peut ainsi définir une action de $\mathrm{Gal}_k(P)$ sur $\mathrm{Rac}(P)$ par

$$\begin{cases} \mathrm{Gal}_k(P) \times \mathrm{Rac}(P) \longrightarrow \mathrm{Rac}(P) \\ \qquad (\sigma, x) \qquad\quad \longmapsto \sigma(x) \end{cases}$$

Le morphisme de groupe associé à cette action permet alors de définir un morphisme de groupes $\mathrm{Gal}_k(P)$ dans $\mathfrak{S}_n$. De plus, ce morphisme est injectif (c'est-à-dire l'action est fidèle) puisque $D_k(P)$ est engendré par les x_i.

Ainsi $\mathrm{Gal}_k(P)$ s'identifie à un sous-groupe de $\mathfrak{S}_n$.

Action transitive et irréductibilité

Lemme Soit $P \in k[X]$ un polynôme dont tous les facteurs irréductibles sont séparables. Le groupe $\mathrm{Gal}_k(P)$ agit transitivement sur les racines de P si et seulement si P est une puissance d'un irréductible.

Si P est une puissance d'un irréductible Q et x, y deux racines de P donc de Q dans $D_k(P)$. Il existe un morphisme τ de $k(x)$ dans $D_k(P)$ qui envoie x sur y. Comme le polynôme P est scindé dans $D_k(P)$, on peut prolonger τ en un (auto)morphisme σ de $D_k(P)$. Ainsi, il existe $\sigma \in \mathrm{Gal}_k(P)$ tel que $\sigma(x) = y$.

Si P n'est pas une puissance d'un irréductible, P admet deux facteurs irréductibles premiers entre eux P_1 et P_2 qui n'ont donc de racines communes dans aucune extension (en effet, il existe $U, V \in k[X]$ tel que $UP_1 + VP_2 = 1$). Si x est une racine de P_1 et y une racine de P_2 dans $D_k(P)$, un élément de $\mathrm{Gal}_k(P)$ enverra x sur une racine de P_1 et donc ne l'enverra jamais sur y.